RSAC 2025 Conference

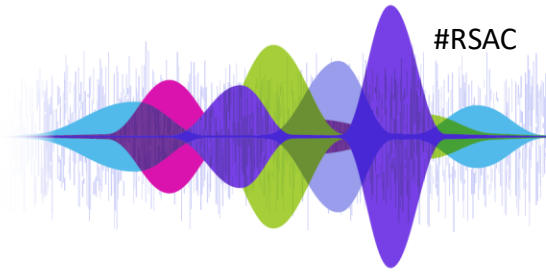
Many Voices.
One Community.

SESSION ID: CSO-R05

Security Relationship Management: Tips to Align Security to the Business

Lee Parrish

Vice President, Chief Information Security Officer
Newell Brands
LinkedIn/In/lee-parrish



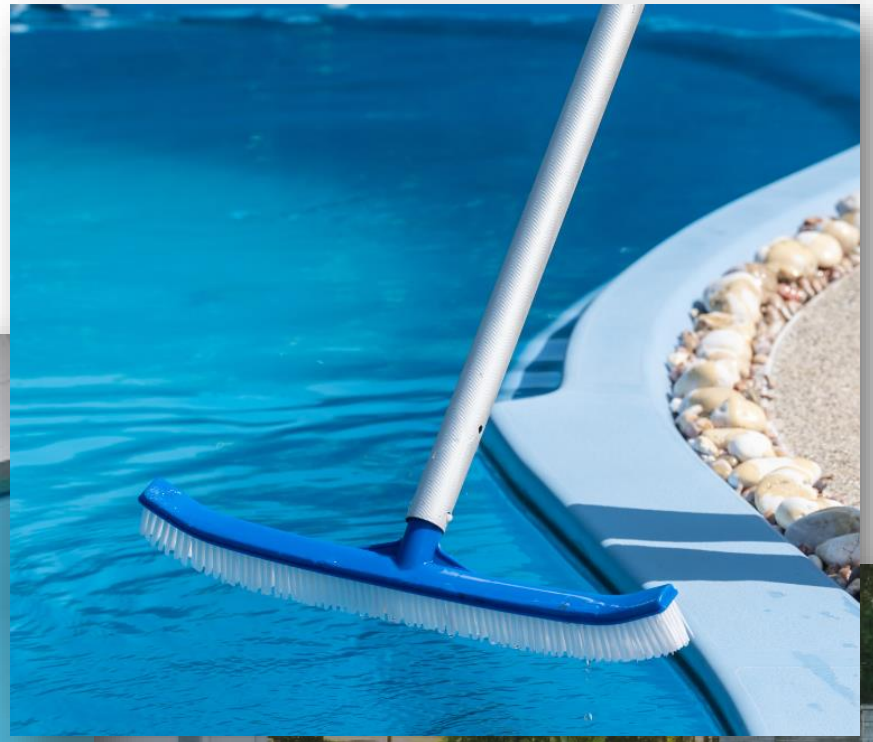
Disclaimer

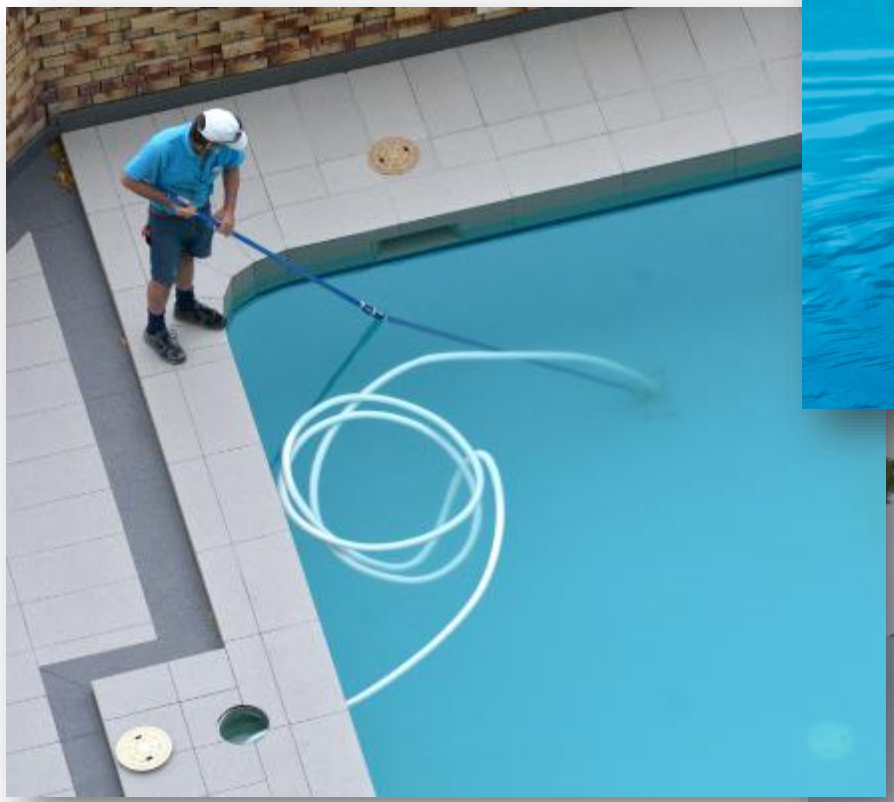
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

5.0
RATING



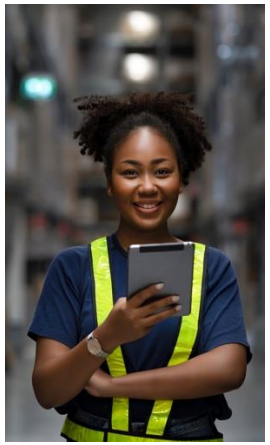


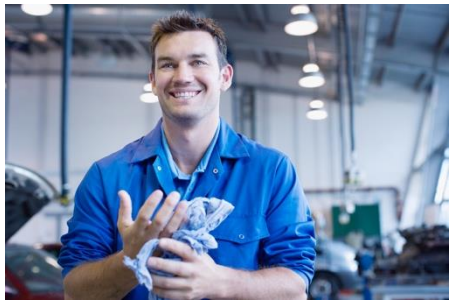
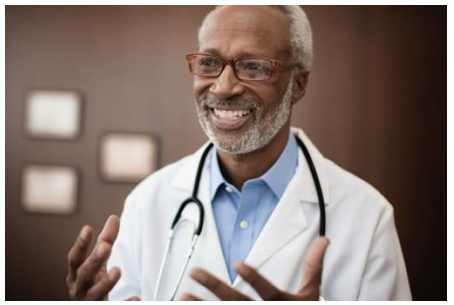
The Issue with General Alignment

- One Enterprise
- Different roles
- Varying goals
- Unique risks

==========

1 Security message

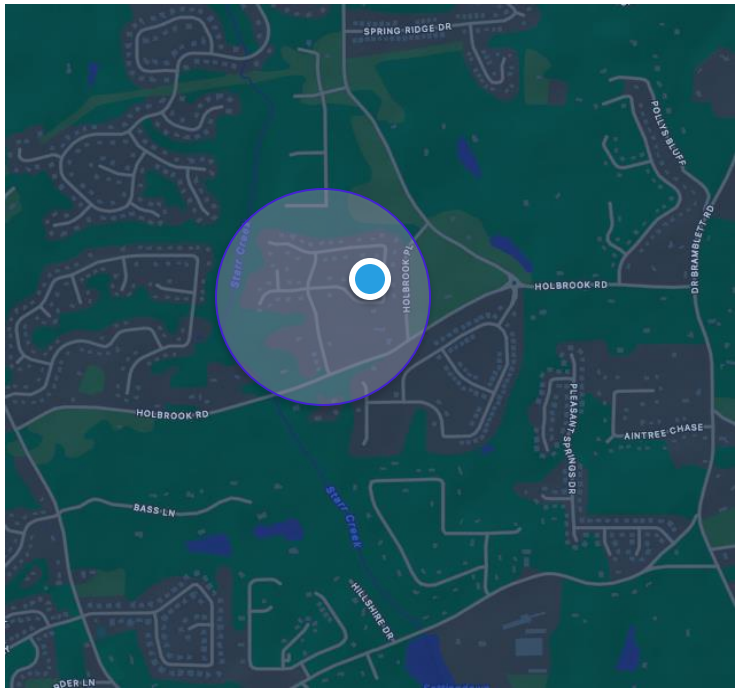


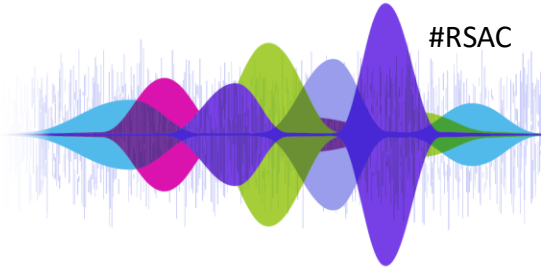
What is “the business”?

Our Goals: A Better Way to Align

- Relevancy is key; making it personal to the receiver
- Leverage marketing concepts to better align our services to wants and needs
- Get close to the “customer” (local information)
- Address the dynamic nature of our business relationships



Our Time Together Today



- Basic marketing concepts we can use
- Introduction to Security Relationship Management (SRM)
- SRM Analytics
- Addressing SRM Challenges
- Implications to the CISO role
- Q&A

Borrowing from our Marketing Friends

- The Four P's
- Customer Relationship Management
- Segmentation (not the network kind)

- Already established processes
- Faster implementation
- Allows for us to focus on security
- "Creative flexibility"

The Four P's

- Assumptions
  - "Creative Flexibility"
  - Applicability to an internal InfoSec program
  - Places us in a ***market-driven*** mindset. For-profit security companies: leverage the 4 P's as intended.

Product

Price

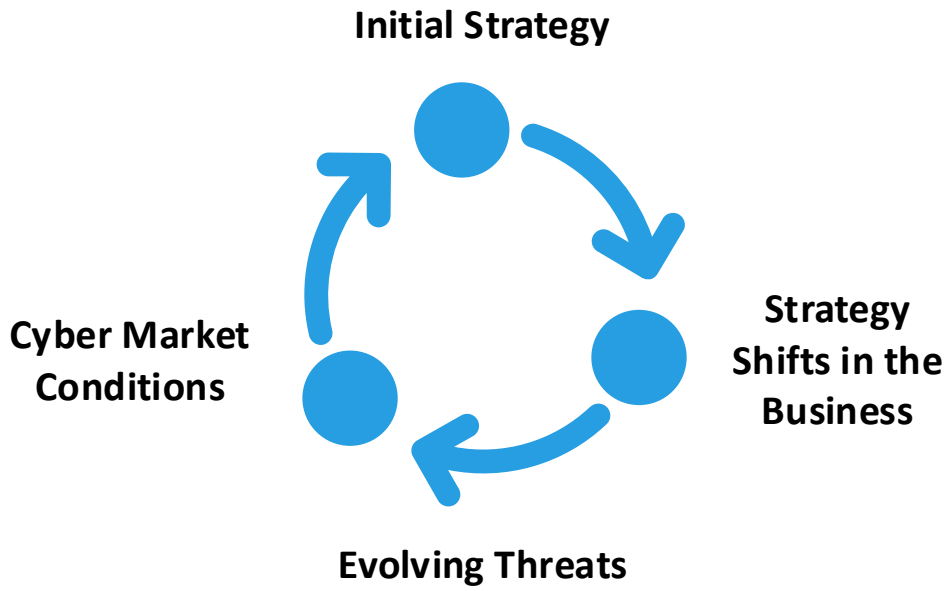
Place

Promotion

Product

A deep & ongoing analysis of your security products & services:

- Fulfill a demand/address a risk
- Address considerations:
  - Available budget
  - Unique risks to your organization
- Quality differentiation
  - Internal vs. external sourcing
- Platform or point solution or hybrid



Price

The “price” issue for an internal program

- Analysis of the ”competition” between external security providers vs. internally sourced services
- Allocation and pay-per-service models
  - Online purchasing & shipping cost example
- Cost transparency

Benefits

- Aligns with the realities of the corporation:
  - Gross profit expansion
  - Bottom-line efficiencies: drive profitable revenue
- Capacity and resource management

Place

- When, where, and how we deliver our services
- Places our services where the consumer would expect to easily find them, when they are needed
- Common practice: ticketing system
- Consider alternate and unofficial channels
- Service catalogs as a recommendation

Promotion

- What are we promoting? Our programs or the security message?
- Wants and Needs
- The Power of Brands > A Test for You
- Building Your Program Brand (logos, gear)
- Promoting:
  - Open House
  - 5/55 Rule
  - Champions Program as “Influencers”

InfoSec Champions Program

Customer Relationship Management

- Grow & manage long-term customer relationships through local information

- CRM is not solely a tool
  - A CRM blast from the past
  - Data Loss Prevention as an example
  - Build relationships: Strategic Alliances example

- Cybersecurity sales
  - Transactional vs. extension of our team

Maintaining Relationships in Our Personal Lives

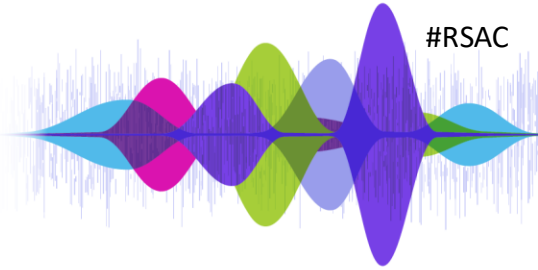
- Spouse/Partner/Significant Other
- Children
- Pets
- Clubs & Recreation
- Parents/Grandparents
- Church

Maintaining Relationships in Our Professional Lives

- All lines of business, sectors, business units
- Functional areas
- The InfoSec team
- 3rd party relationships
- Industry contacts

Organization is a must to keep up with our relationships

Purpose of Segmentation



- A pathway to targeted communications
- Segment (divide) the enterprise into manageable sub-groups with similar attributes
- Enables opportunities to develop unique cybersecurity messages
- Listen to what is top of mind for each segment and craft the message accordingly
- Your segmentation strategy should be customized to your environment

Suggested Segments

- Differentiate, but keep manageable
- Allow for flexibility as business evolves

Did I Miss Any?
Of Course - Customize to Your Needs

Your Organization

Lines of Business/Hospitals/Energy Divisions
Board of Directors
Executive Team
Committees (InfoSec, Disclosure, etc.)

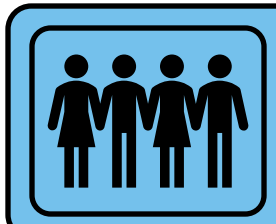
Functional Areas

Human Resources
Manufacturing
Internal Audit
Investor Relations
Legal
Finance
IT (& InfoSec)
Comms

External Relationships

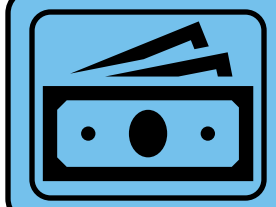
Vendors
External Auditor
Cybersecurity Industry
Outside Counsel
Advisory Boards

Core Attributes of Segments



Key Stakeholders

- Not all people within a segment
- Not just leaders

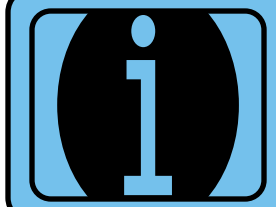


Segment Contributions

- % of overall revenue
- Qualitative contributions

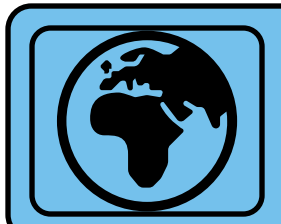
Metrics & Measurements

- InfoSec requests – segment involvement
- Segment-specific security metrics



Segment Details

- Product lines/Services
- Locations

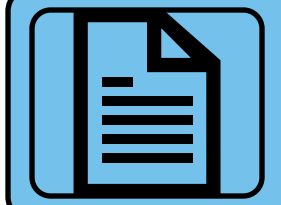


Cultural Considerations

- Interpretation of terms, language
- Internal cultural factors

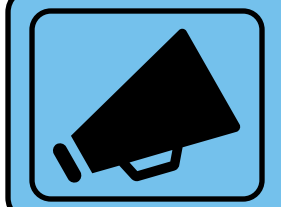
Compliance Requirements

- Unique requirements for segment
- Healthcare data, payment card info, etc.



Documentation Retention

- Store notes from interactions
- Presentations to and from the segment



Feedback Loops

- Processes for gathering feedback
- Requires constant collection & evaluation

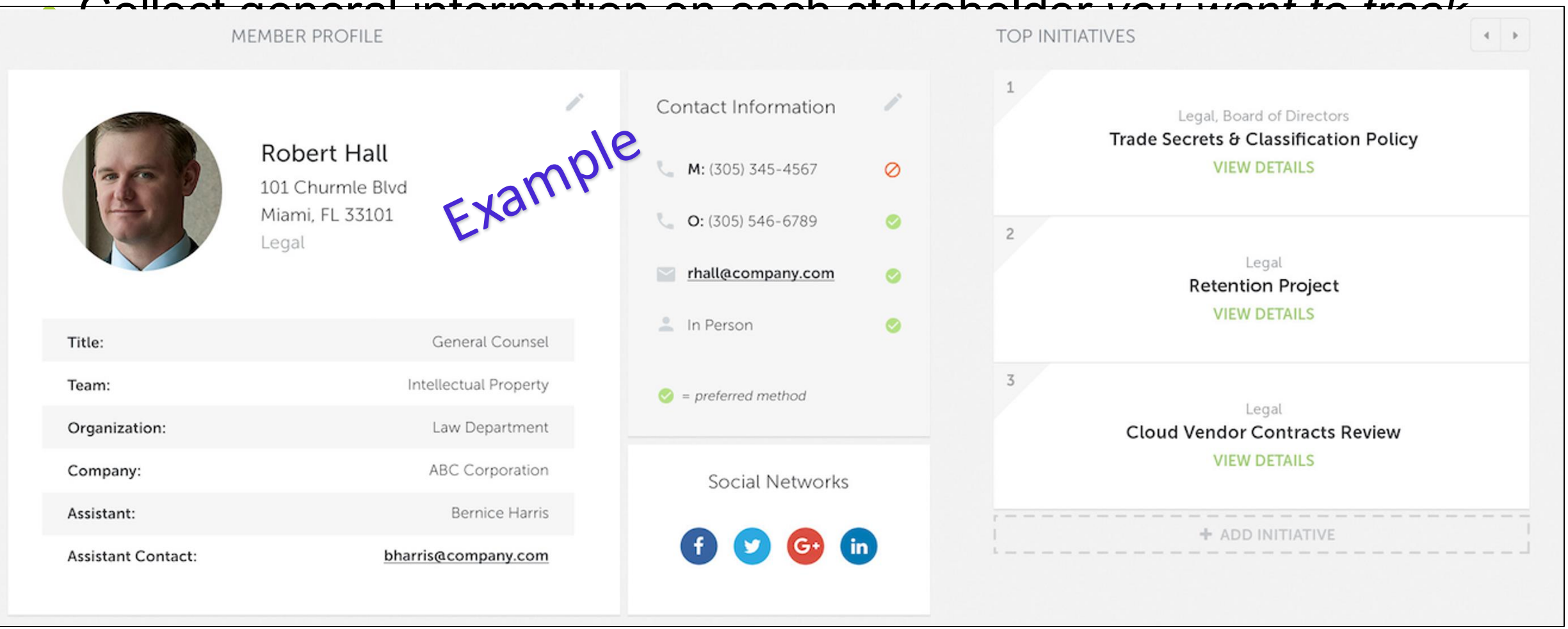
An Introduction to Security Relationship Management

Goal: build a bi-directional communication strategy for your cybersecurity program by building strong relationships across all segments of your company to promote your “brand”.

- Borrows concepts from CRM and segmentation; adjusted for cybersecurity.
- Measure and manage these relationships with tracking data based on various attributes of interactions.
- Garner feedback and “local information” of each segment to better understand corporate strategies/opportunities.

Segment/Key Stakeholder Information

- Collect general information on each stakeholder you want to track

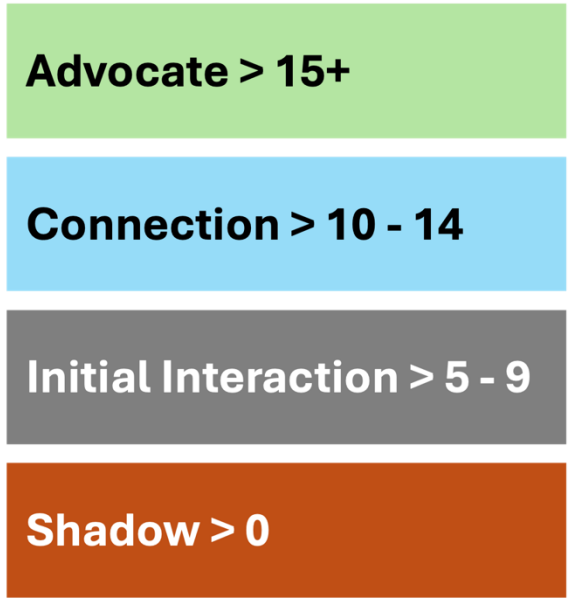


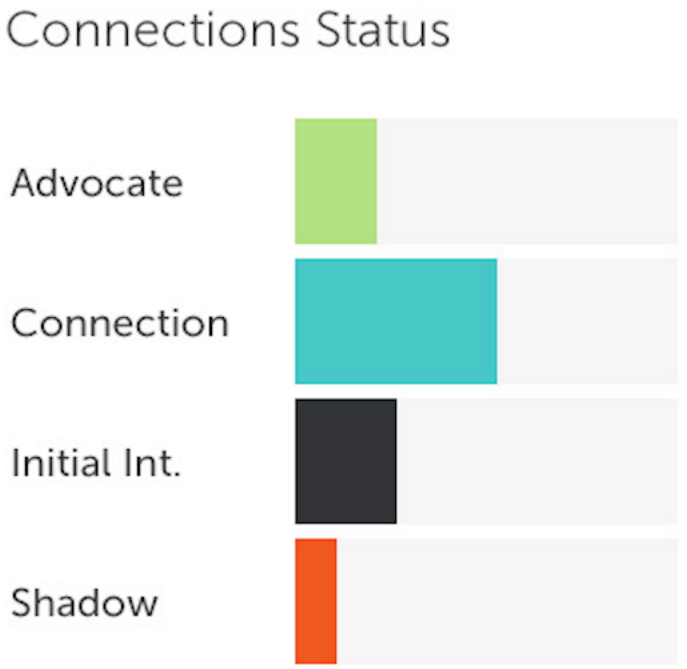
Engagement Type	Description	Points
Email/Text	Originator of email/text or responding to an email/text between the CISO and the stakeholder only	1
Phone - Group	More than two participants on the call	2
Phone – 1:1	1:1 phone call with stakeholder	5
Meeting – Virtual – Group - Presentation	Attending a virtual meeting with a one-way delivery of content to participants without much interaction	3
Meeting – Virtual – Group – 10+	Attending a virtual meeting with ten or more participants in which there is interaction	4
Meeting – Virtual – Group – 3+	Attending a virtual meeting with three to nine participants in which there is interaction	5
Meeting – Virtual – 1:1	Attending a one-on-one virtual meeting	8
Meeting – In Person – Group – 10+	Attending an in-person meeting with ten or more participants in which there is interaction	6
Meeting – In Person – Group – 3+	Attending an in-person meeting with three to nine participants in which there is interaction	7
Meeting – In Person – 1:1	Attending an in-person one-on-one meeting	10
****In-Person Offsite Multiplier Bonus**	For in-person meeting types held offsite, away from the corporate office, add a 2x multiplier to the standard points	2x

SRM Analytics: Tiers

- Total # of monthly points for each segment or stakeholder determines their tier.

- Goal: elevate your connections' tier levels with high quality interactions.

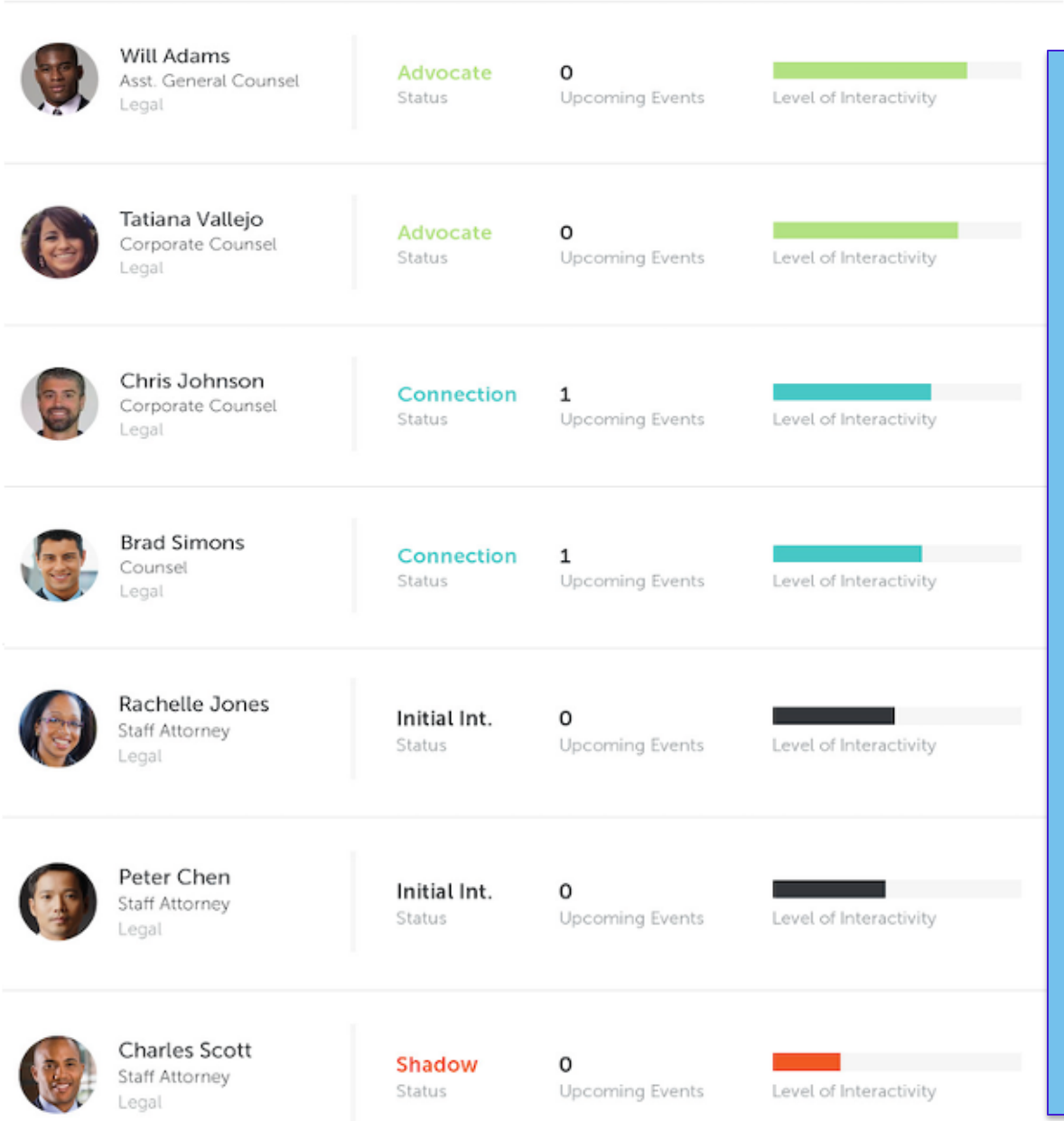




SRM Analytics: Monthly Review

- The monthly review is critical to ensure adequate attention is given to all your stakeholders.
- The higher the tier = more relevancy + more alignment.
- Dynamic process, measure accordingly. Subtract points for inactivity.

The monthly review looks at all your stakeholders to review who are advocates, who are in the shadow tier, and all levels in between.



Use the data from your monthly reviews to create actionable plans to increase interactions where they are needed most.

SRM Analytics: Example

General Counsel

General Counsel Interactions – Previous Month

- 2 One-on-One meetings – video (8x2=16 points)
- Follow-up phone call with a question (5 points)

Total 21 points for previous month – Advocate Tier

General Counsel Interactions – Current Month

- None (subtract 10 points) 11 points – Connection Tier

External Relationships

- You've probably made some this week
- Security vendors
  - Extensions of your team
  - Market entries
- Regional meet-ups
- Advisory boards

- Outside Counsel
- External Auditors

Need to Alter Your SRM Analytics to Address Frequency Needs

RSAC 2025 Conference

Potential SRM Challenges

And how to address them…

Many Voices.
One Community.

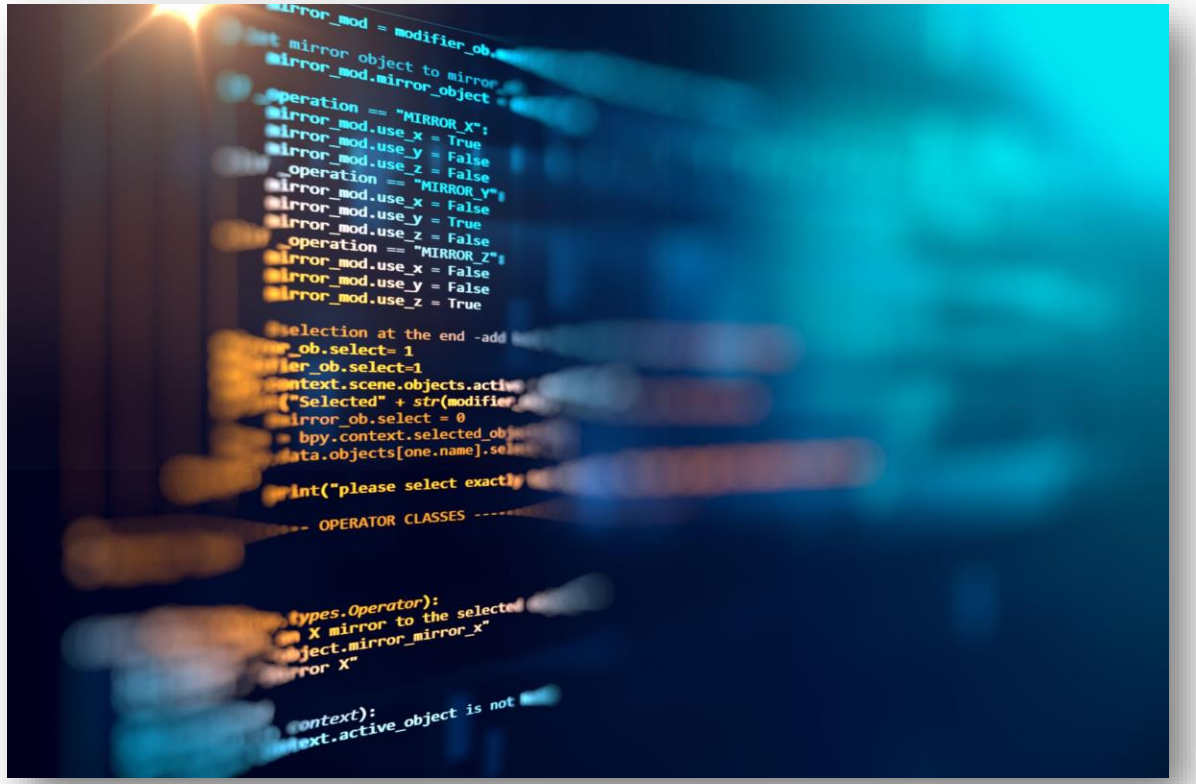
Potential SRM Challenges

- C’mon man…. This is a lot of work.

We spend so much time tracking the technical attributes of security:

- Vulnerability management
- Pen testing findings
- Endpoint detection data
- Security awareness metrics

Your relationships require the same attention.



Use customized security data that is applicable to the segment you’re speaking to

Potential SRM Challenges

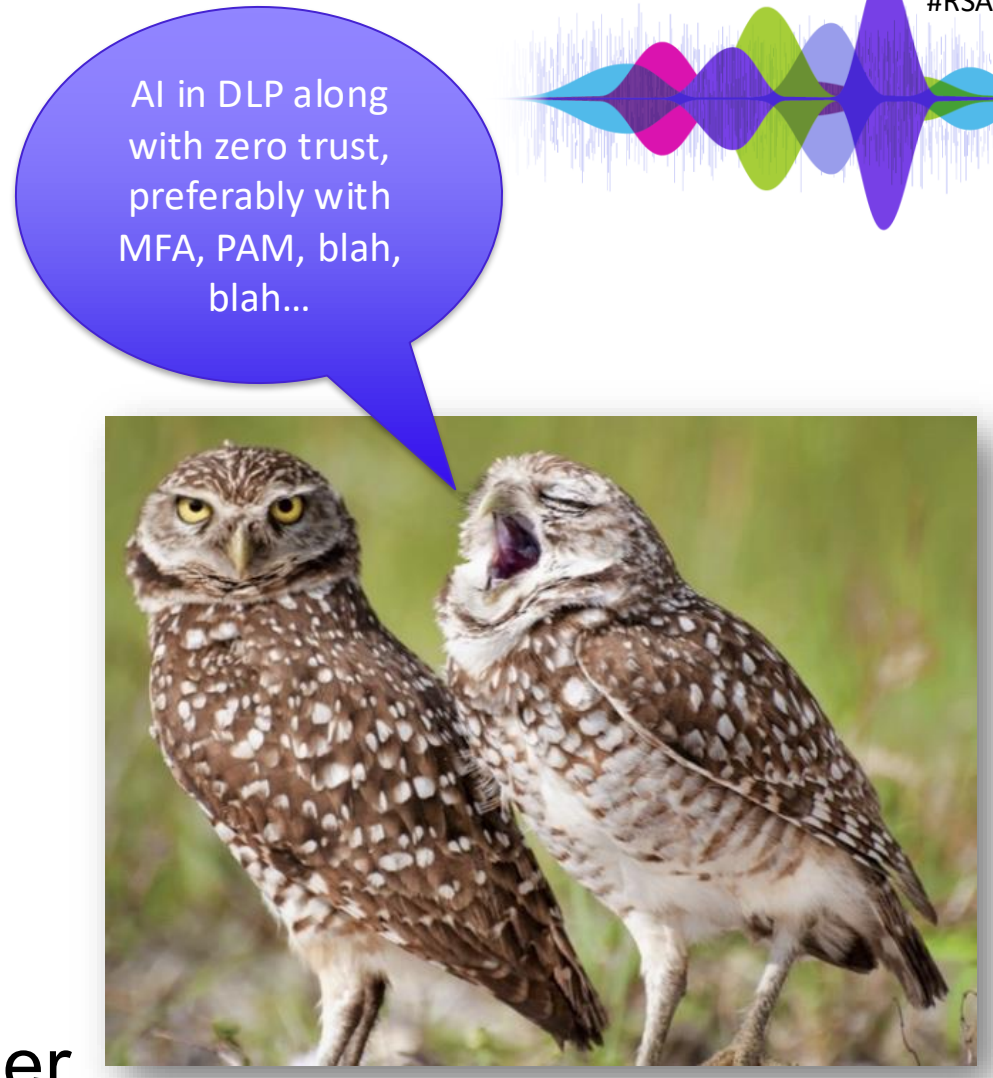
Lack of Willingness to Engage - Blockers

- May have pre-determined ideas on security (good or bad)
- Doesn't fully recognize the relevancy of cybersecurity
- Bigger fish to fry in their own segment
- Just don't have the time

Potential Methods to Address Blockers

- ✓ Establish relevancy through *wants & needs*
  - ✓ Something to help in their duties & sophisticated level of FUD
  - ✓ Increased compliance to regulations
- ✓ Use advocates as allies – introductions, shares your value
- ✓ Be present; walk the halls

Potential SRM Challenges



Oversaturation & Balancing the Message

- Replace the focus of length of interactions with the quality of the interaction
- Tailor your interaction to your stakeholder
  - Executive
  - Technical expert
  - Finance professional
- Leverage your SRM analytics to balance tier expansion with saturation

Potential SRM Challenges

Geographical Considerations

- Travel budget challenges
- Time zone differences
- Balance local support with enterprise initiatives (in a centralized model)
- ✓ Occasionally alternate meeting times to accommodate schedules
- ✓ Even low value interactions (email, chat) are useful when face-to-face is not available

Potential SRM Challenges

Company size too small

- My company is a small, regional company. I literally know everyone. Do I really need SRM?

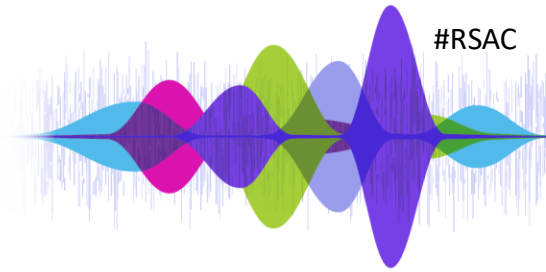
✓Yes, because:

  - May have tighter budgets
  - Collaboration to squeeze out efficiencies is vital
  - Tracking interactions remains important to understand current topics, prevent oversaturation, retain discussion points/documentation
  - We still have numerous external relationships to manage

RSAC 2025 Conference

Implications to the CISO Role

CISO Role Implications



The Importance of our Discipline

- Enterprise Risk Mgmt.
- Regulatory (10K, etc.)
- Breach impacts on the business

Enterprise Reach

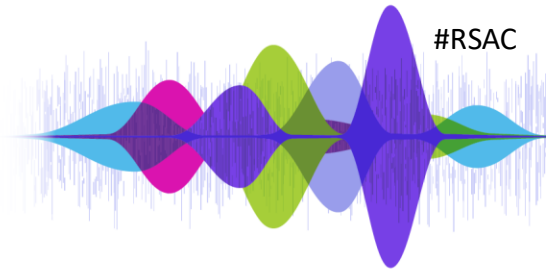
- Responsibilities don't end at the IT organizational boundary
- Unique visibility into the business
- Other committees

Executive Level Access

- More of a fixture in executive conference rooms and boardrooms
- Execs: business resiliency
- Board: oversight

External Factors Largely Outside of the CISO's Control

All That's Left to Elevate the CISO Role: Internal Factors

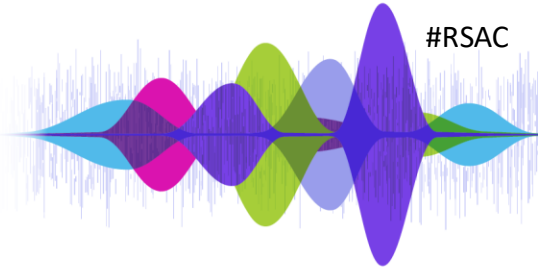


The emergence of the three external factors positions the CISO to contribute to other strategic decision-making areas of the business.

- Address internal factors (that we can control) to contribute more to the company's strategic direction – alignment helps us to do this.

- Or alternatively, rely on an executive proxy to translate the technical strategies into business terms on our behalf.

Apply What You Have Learned Today



- Next week you should:
  - Review your security strategy to ensure you covered the Four P's with a "market-driven" lens
- In the first three months following this presentation you should:
  - Plan your Security Relationship Management Program, points/tiers
  - Identify your segments, the core attributes, and other info you want to capture
- Within six months you should:
  - Begin tracking your interactions
  - Ensure you complete a monthly review of your SRM performance

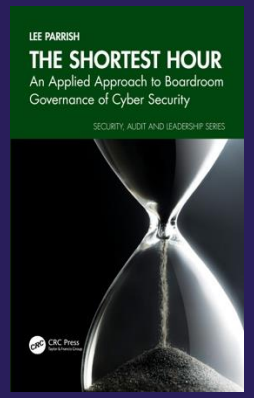
RSAC 2025 Conference

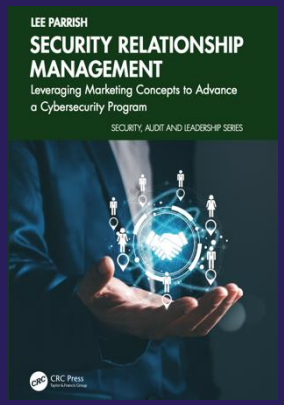
Many Voices.
One Community.

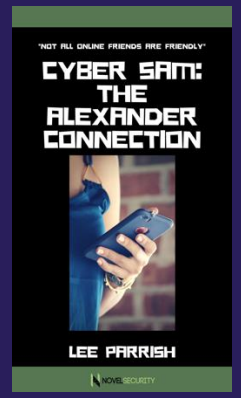
Thank You!

For More Information:

LinkedIn


LEE PARRISH
THE SHORTEST HOUR
An Applied Approach to Boardroom Governance of Cyber Security
SECURITY, AUDIT AND LEADERSHIP SERIES
CRC Press


LEE PARRISH
SECURITY RELATIONSHIP MANAGEMENT
Leveraging Marketing Concepts to Advance a Cybersecurity Program
SECURITY, AUDIT AND LEADERSHIP SERIES
CRC Press



Novel Security